REMARKS

Reconsideration and reexamination are respectfully requested in view of the below remarks.

Rejections under 35 U.S.C. §103

Claims 1-3, 6-7, 9-10, 13-14 and 16 were rejected under 35 U.S.C. §103(a) as being unpatentable over Hoke et al. (US pat. 6,701,437) in view of Hama (US 7,072,346).

Independent claim 1 recites:

A method of securing packet data transferred between a group of stations over on a backbone, the backbone comprising an ingress point and egress point, the method comprising the steps of:

receiving, at the ingress point of the backbone, group security association data associated with the group of stations;

receiving a packet at the ingress point of the backbone, a packet including **a group identifier** corresponding to the group of stations and a destination address for the packet;

transforming, at the ingress point of the backbone, the packet **according to the group security association associated with the group identifier**; and

forwarding the transformed packet over the backbone **using the group identifier** as a backbone address.

Thus in the present invention a group identifier is associated *both* with the transformation of the packet *and* with the forwarding of the transformed packet at the ingress point of the backbone. With such an arrangement the packet can be secured across the backbone via trusted ingress and egress points of the backbone that have knowledge of the group by using the group identifier to associate a packet both with group security transforms as well as group forwarding information. Scalability issues are addressed because the number of VPNs across the backbone is no longer associated with discrete end-points, but rather with groups of end-points.

Hoke:

Hoke describes, at col. 3, lines 29-20:

"... a virtual private network (VPN) unit for selectively processing secure communications for members of a virtual private network. One embodiment of the present invention is used in a VPN operating over a public data network connected to an organization's private network (e.g., a LAN or WAN). The organization's private network includes one or more end stations that are members of the VPN. In this first embodiment, a VPN unit serving the VPN member end stations contains a processor, storage memories, and a communication port. A method of configuring the VPN unit is also provided, whereby VPN communications (e.g., communications requiring secure transmission between members of a VPN) are processed by the VPN unit but other communications bypass it..."

A VPN unit of Hoke, as described at column 4 lines 45-48, receives configuration parameters that are used to configure the VPN unit to appropriately handle communications between members of VPNs. As described at column 8, lines 37-43:

"...VPN units maintain lookup tables for ***identifying members of specific virtual private networks*** and groups within a particular virtual private network. When VPN traffic is sent between source and destination end stations that are both members of the same VPN, the VPN unit serving the source end station processes the data packet, encrypts it, compresses it (if necessary), and adds authentication information as needed..."

Thus, the VPN unit maintains lookup tables that identify both ***end stations*** to figure out the appropriate transformation to apply to the packet. Transformations are done at the end stations ***prior*** to forwarding it elsewhere in the network. Such a structure is described in the Background of the Invention section of Applicant's specification at page 4. One drawback of such a structure is the difficulty of scaling such a solution since the VPN unit must maintain security association information for each source/destination pair.

In contrast, the claimed invention discloses the use of a VPN *group* identifier (as opposed to a source/destination pair). The VPN-ID is used to determine a transform to apply to the packet as well as providing a tag for routing across the backbone.

The Examiner states, at page 3 of the office action:

> "... Hoke fails to teach the packet including a group identifier and a destination for the packet. However, Hama teaches receiving packet including a group identifier and a destination for the packet (Hama, column 10, lines 25-53, destination address contained in the packet when packet enters.... VID contained in tag). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Hama's method of using group identifiers because it offers the advantage of allowing terminals belong to the same VLAN to communicate with each other regardless of where they are installed (Hama, column 2 lines 4-20)..."

Hama:

Hama describes, in the Abstract:

"... In network for forming a VPN on a shared network and communicating via the VPN, a core network of the VPN is formed by an MPLS network, access networks for accessing the core network are formed by VLANs, and edge routers are provided between the MPLS network and VLANs for interfacing the MPLS network and the VLANs. A transmit-side edge router converts a packet, which enters from a VLAN, to an MPLS packet and transmits this MPLS packet to the MPLS network, A receive-side edge router converts the MPLS packet, which has been received from the MPLS network, to a VLAN packet and directs the VLAN packet to a VLAN that belongs to the same VPN as that of a VLAN on the transmit side...."

Hama describes, at column 9 line 62 – column 10 line 12:

"...More specifically, the transmit-side edge router converts a VID contained in a VLAN packet to a VPN label, which is a VPN identifier, finds a forwarding label for forwarding the packet along a prescribed route on the basis of the destination of the VLAN packet, imposes these labels in place of the VIN to generate an MPLS packet, and sends the MPLS packet to the MPLS network 110. The latter routes the MPLS packet to the target receive-side edge router over a preset route while the forwarding label of the packet is replaced. Upon receiving the MPLS packet from the MPLS network, a receive-side edge router removes the forwarding label, converts the VPN label to the original VID, adds this VID to the packet in place of the label to generate a VLAN packet and sends the VLAN packet to the VLAN indicated by the VID. As a result of this operation, a packet can be transmitted from a transmit-side VLAN belonging to a certain VPN to a receive-side VLAN belong to the same VPN..."

Therefore in Hama, there is no teaching or suggestion of using the group identifier both for routing across the backplane and for ***transforming*** the packet. Rather, Hama describes that packets received at the edge router have *already* been transformed and encapsulated with a VID label, and this VID label is used to generate a VPN label. Thus Hama fails to overcome the problems of scalability of Hoke, which requires large lookup tables to be maintained at each VPN end point.

Neither of the prior art references address the scalability issue of VPNs. The present invention, in contrast, provides a significant advantage in scalability over the combined solution of Hama and Hoke by moving the application of security transforms associated with a group to *trusted ingress points,* routing across the backbone using the group identifier and decoding the transforms at the egress point, using the same group identifier to determine the appropriate decode to apply to the transform. With such a result, the amount of information that needs to be stored at ingress and egress points is drastically reduced, even in the event that a large number of VPNs traverse the backbone. Such advantage in scalability is not realized by the combination of Hama and Hoke.

Applicants note that they have amended the claims to more particular claim that the ingress node is a provider edge device. As described at page 20 of Applicant's specification, it may be desirable to have a trusted service provider perform the transformation of the packets using this method. Applicants have amended the claims to incorporate the limitation of claim 5 into claim 1, to more particularly claim this aspect. Applicant's note that such a teaching is in direct contrast with that of Hoke, which describes with regard to Figure 3 of Hoke that packets are secured *before* they are forwarded to a provider. Accordingly, Applicant respectfully submits

that one would not be motivated to modify Hoke, Hama or the combination thereof to reach the limitations of the claims in view of the teachings of Hoke.

Accordingly, for at least the reason that the combination of Hama and Hoke fails to describe or suggest "...receiving, ***at the ingress point of the backbone, group security association*** data associated with the group of stations ... receiving a packet at the ingress point of the backbone, a packet including a group identifier corresponding to the group of stations and a destination address for the packet ... ***transforming, at the ingress point of the backbone, the packet according to the group security association*** associated with the group identifier; ***and forwarding the transformed packet over the backbone using the group identifier as a backbone address***..." it is requested that the rejection be withdrawn. Dependent claim 2 serves to further limit claim 1 and is therefore allowable with claim 1.

Claim 6, as amended, now recites the steps of "…receiving a packet at the egress point of the backbone, ***wherein the egress point is a provider edge device***, *the packet including an identifier of the group of stations and a destination for the packet* … restoring the packet responsive to the group security association data associated with the identifier of the group of stations; and forwarding the packet to the destination…"

Accordingly, claim 6 includes limitations similar to those of claim 1, in particular the use of a packet that includes an identifier of a group of stations in addition to a destination address. The claims is patentably distinct over Hoke and Hama for the reasons described above, in particular that the references fail to disclose that the transformation is performed at the provider

edge device. For at least the reason that the combination of Hoke and Hama fails to teach or suggest every limitation of claim 6 it is therefore requested that the rejection be withdrawn.

Claim 10, as amended, now recites "…an ingress point to the communication link wherein the communication link comprises a plurality of provider devices, and **wherein the ingress point is one of the plurality of provider devices** ..... a group security association, corresponding to a group of stations in a private network, both the first station and the second station being members of the group and wherein a group identifier is associated with the group; .... **means for securing data transferred between members of the group from the ingress point** and the egress point in the network using the group security association **by transforming the data at the ingress point using a group security association associated with the group identifier;…**" As described above with regard to claim 1, no such structure is shown or suggested by Hoke, Hama or the combination thereof and it is therefore requested that the rejection be withdrawn. Dependent claims 12, 13 and 16 serve to further limit claim 10 are therefore allowable with claim 10.

Rejections under 35 U.S.C. §103

Claims 4-5, 8, 12 and 15 were rejected under 35 U.S.C. §103 as unpatentable over Hoke and Hama and further in view of Mukherjee, U.S. Patent Application No. 2004/0006708.

Applicants note that claims 4-5, 8, 12 and 15 have been cancelled, although elements from some claims were moved to independent claims. Thus Applicant's will still address the Examiner's concerns below.

Mukherjee:

Mukherjee describes, in the Abstract:

"A method for providing peer-to-peer virtual private network (P2P-VPN) services over a network. The method includes identifying subnet and host addresses for each user device requesting participation in a virtual private network (VPN) session. Once the subnet and host addresses are identified, a virtual private host (VPH) is initiated for each user device, where each VPH communicates with each user device via a respective tunnel through the network, thereby enabling secure communications between the user devices..."

Thus, Mukherjee, like Hoke and Hama associate VPN end points to end users. In contrast, the concepts of the present invention extend the end points to be trusted ingress and egress points, some of which may be provider devices. Hoke, Hama and Mukherjee, which each teach a tight association between VPN end-users and VPN end points, neither disclose nor suggest the claimed invention, but rather present solutions which have scalability issues. Accordingly it is respectfully requested that the rejection using these references be withdrawn.

Conclusion:

Applicants have made a diligent effort to place the claims in condition for allowance. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Applicants' Attorney at the number listed below so that such issues may be resolved as expeditiously as possible.

For these reasons, and in view of the above amendments, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,

August 22, 2007 ____/Lindsay G. McGuinness/_____

Date

Lindsay G. McGuinness, Reg. No. 38,549
Attorney/Agent for Applicant(s)
McGuinness & Manaras LLP
125 Nagog Park
Acton, MA 01720
(978) 264-6664

Docket No. 120-142
Dd: 8/19/2007